有利資料

李國誠 Guo-Cheng, Li

Education

國立臺灣科技大學 資訊管理系 四年級　　輔系:資訊工程系(能夠修習資工系資安課程)

September 2019 — June 2023

GPA : 4.11 (原始成績 93.03)　系排: 7 %　-------- 資安科技與管理學程(剩一門修畢)

Experience

Electronic voting system based on Physically Unclonable Function

第 32 屆全國資訊安全會議發表 (2022 CISC) 第一作者

June 2022

- Hardware - encrypted
- SRAM Physically Unclonable Function (SRAM PUF)
- Hash Function – SHA-256

專題 - 科技部大專生計畫

July 2022 — February 2023

- 工程技術司
- 計畫編號: 111-2813-C-011-007-E

資訊工業策進會 資安科技研究所 聯網安全暑期實習計畫 優等

July 2022 — September 2022

- 研究專題 : IoT Zeroday
- 地震儀物聯網漏洞 – 利用 Local File Inclusion (LFI) 漏洞來進行白箱測試
- Command Injection, Arbitrary File Upload, Logic Flaws, Privilege Escalation (CVE-2021-4034)

AIS3 新型態資安暑期實務培訓 學員

July 2022

- 車載安全組
- 專題: CAN bus 模擬劫持 – 模擬車輛電子訊號進而劫持並操控車輛

第 26 屆全國資訊服務創新競賽 資安組決賽

September 2021 – November 2022

- Information Security Category - Final

第七屆臺灣好厲駭 資安培訓計畫 高階培訓學員

September 2022 – August 2023

KPMG 安侯企業 數位安全部 資安技術研究員

September 2022 – June 2023

- 軟體逆向工程，網頁元件動靜態分析滲透測試

研究計畫 - 國立臺灣科技大學資訊管理系四年級 李國誠

預期研究方向: CDN (Content Deliver Network) 技術下的資訊安全

1. 研究動機

網際網路如今已經佈滿在我們的生活當中，時間的推移下網路架構也隨之增多，不僅僅是為了增加傳輸效率，更可以防止某些特定惡意攻擊。正是因為不停的有新興架構的產生，網路資訊安全研究並不會因為隨著時間而停止。在近幾年陸續有人針對內容傳遞網路 CDN (Content Deliver Network) 的資訊安全提出疑慮，CDN 技術的確能提供高質量的 QoS (Quality of Service)，但在提高用戶使用體驗的同時也產生出了諸多可造成的攻擊手法，期許透過研究 CDN 的網路架構結合貴所課程規劃、資源以及教授的指導下能降低 CDN 架構產生的攻擊問題。

2. 研究背景

內容傳遞網路 CDN (Content Deliver Network) 與傳統單一節點網站服務模式的網路架構相比下，能夠有效提高瀏覽速度、前端點防護、節省靜態流量以及隱藏真實伺服器端 IP address，在攻擊面向中最有效的方式就是直接攻擊源伺服器端，但因多數 CDN 架構會有 WAF (Web Application Firewall) 去阻擋一些惡意流量，在攻擊手法上無法輕易繞過，所以需先了解整個網路架構能造成的攻擊面向才能研究出有效的防禦機制。

3. 文獻探討

3.1 Content Deliver Network, CDN

CDN 是一種分佈式網路架構，由大量節點伺服器組成，原理是引導使用者到最近的伺服器並通過有效的實現負載均衡的管理機制，CDN 技術不僅僅可以減少用戶端到端的延遲，還減輕了內容提供的負擔，更可以減低分散式阻斷服務（DDoS）攻擊。

CDN 工作流程[2]:

1. 當用戶端訪問 CDN 網站時，DNS 伺服器將開始 DNS 解析。
2. DNS 解析將指向 CDN 的 DNS 伺服器。
3. CDN 的 DNS 伺服器根據請求重定向機制向用戶端返回一個邊緣服務器。
4. 用戶端訪問給定的最近邊緣服務器。該機制的特點是就近判斷和重定向過程發生在用戶請求 DNS 解析的那一刻而不是服務器連接的時刻。
5. 當請求被重定向到邊緣服務器時，邊緣服務器將使用其內部的本地負載平衡算法為用戶端分配合適的緩存服務器。
6. 用戶端從分配的緩存服務器獲取請求的內容。如果請求的 Web 內容未緩存在其上，則將從內容提供者源服務器獲取內容。

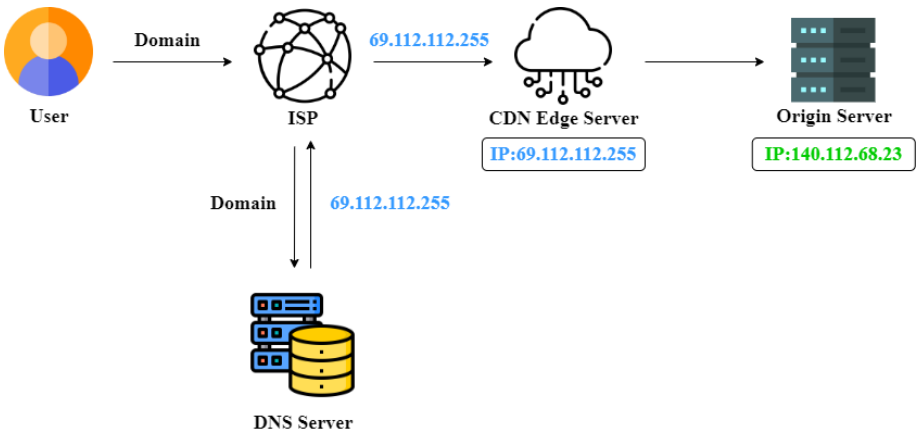


圖 3-1 CDN 原理 來源:自行繪製

3.2 Web Application Firewall, WAF

Web 應用程式防火牆可協助保護 Web 應用程式免於遭受惡意攻擊和不必要的網際網路流量，包括機器人、注入和應用程式層拒絕服務 (DoS)。WAF 解析與比對病毒、惡意程式等網路威脅，加強防禦 DDoS 攻擊、SQL 注入、XML 注入、XSS 等應用層 (Layer 7) 入侵。

3.3 Domain Name System, DNS

DNS 協議用於通過解析遵循分散分層命名系統的域名來查找主機 IP。 DNS 的穩健性和可靠性使其成為現今互聯網基礎設施中最關鍵的組件之一。DNS 在 UDP 的 53 端口上進行查詢，並使用 TCP 在主 DNS 服務器和輔助 DNS 服務器之間進行區域傳輸。它是一種網絡協議，可將人類可讀的域名（例如 webs.legals.software）轉換為機器可理解的 IP 地址（例如 128.199.103.28）。[5]

3.4 分散式阻斷服務（DDoS）

DDoS 攻擊的基本策略是耗盡受害者的資源，導致目標資源在特定時間內不可用，從而無法將服務交付給合法用戶。在過去數十年中，針對不同組織發起了許多 DDoS 攻擊。大多數 DDoS 攻擊的目標是使服務不可用，從而導致收入損失以及修復服務的成本增加

4. 研究設計

如果想將 CDN 所產生的問題，必先其了解攻擊手法，CDN 分散式的設計使有心人士常用攻擊手法為繞過 CDN 伺服器去尋找源 IP，以下設計攻擊流程如下:

1. 查看其網站是否使用 CDN 服務(CDN 伺服器 IP 為公開的)，有以下幾種方式
   1-1 利用 nslookup IP。
   1-2 使用 dig 查詢域名服務器。
   1-3 Multi Ping。
   1-4 製造網址解析錯誤看 Error information。

2. 尋找源伺服器 IP，有以下幾種方式
   2-1 子/域名探測。
   2-2 查詢過往 DNS 紀錄。

2-3 Subject Alternative Name (SAN)

SAN 是在簽發憑證的時候加上 SAN 的欄位，讓憑證可以符合多個獨立的網域。例如可以簽一張憑證給 ntust.com 跟 ntust.security 一起用，不需要是同一個網域下面的子網域。相對變更 SAN 需要進行重新簽發；另外 SAN 也有一個上限值，不能無限增加網域。

2-4 Domain Fronting

2-5 查看關聯的 Domain

2-5-1 BuildWith: 申請域名、申請紀錄時間軸，最早的 IP 可能是使用 CDN 前的原始 IP。

2-5-2 CloudFlair。

2-6 OSINT

2-6-1 搜尋 whois 資料庫。

2-6-2 特徵搜尋引擎。

2-6-3 TheHarvester。

2-7 其他思路

2-7-1 針對客服功能或後台紀錄 (XSS)。

2-7-2 log4shell (由 log4j 中 lookup 功能所產生的任制執行指令的漏洞)。

2-7-3 Webshell。

3. CF-Connecting-IP 後利用–可偽造。

攻擊流程: 單個 domain -> sublis3r -> subdomains -> nmap -> 真實 IP & port -> 漏洞應用

發現原始 IP 所設計的防禦措施:

1. 白名單允許的 CDN IP。
2. 和目標網站在同一台服務器但開放在其他端口的網站不掛 CDN 的 IP 段差距要大。
3. 用第三方服務平台取代原生網站功能。

以上針對 CDN 所設計的攻擊及防禦手法較偏向實務層面上的流程，其造成影響遠遠不只這些，[4]CDN 提供商可以推斷用戶偏好和流行，從而導致信息洩露。此類信息洩露可能會導致用戶隱私並將業務特定信息透露給不受信任的人或受損的 CDN 提供商，研究上可架設 cachedeception 環境，模擬在短時限內能竊取數百數千位使用者的個人資料數據。

5. 預期成果

透過實際場景的模擬及架設環境測試，期望能針對各種攻擊手法設計出相對應的防禦機制與流程。多次模擬數據分析過程產生的問題與實驗結果，撰寫學術報告亦會撰寫實務性報告以利此機制與流程能利用在未來相關場域當中。

6. 研究規劃

針對規劃做了以下流程:

1. 研讀文獻了解其原理。
2. 建構 CDN 模擬架構。
3. 透過先進們的研究復現其漏洞。
4. 以舊有漏洞建構防禦機制。

5. 嘗試在模擬研究下尋找延伸問題。
6. 提出問題並嘗試證明。
7. 成功針對此架構資安問題設計解決方式並證明。

在規劃當中也許不會順利照著流程走，但期望在過程當中增進研究能力，培養不輕言放棄的決心，在資訊安全領域依然抱有熱忱，也希望在貴所就讀能夠將學術成果成功發表於國際期刊以及能夠在資安活動上與先進們分享。

7. 參考文獻

[1] E. Jalalpour, M. Ghaznavi, D. Migault, S. Preda, M. Pourzandi and R. Boutaba, "Dynamic Security Orchestration for CDN Edge-Servers," 2018 4th IEEE Conference on Network Softwarization and Workshops (NetSoft), 2018, pp. 329-331, doi: 10.1109/NETSOFT.2018.8459970.

[2] Li Ling, Ma Xiaozhen and Huang Yulan, "CDN cloud: A novel scheme for combining CDN and cloud computing," Proceedings of 2013 2nd International Conference on Measurement, Information and Control, 2013, pp. 687-690, doi: 10.1109/MIC.2013.6758055.

[3] K. Kim, Y. You, M. Park and K. Lee, "DDoS Mitigation: Decentralized CDN Using Private Blockchain," 2018 Tenth International Conference on Ubiquitous and Future Networks (ICUFN), 2018, pp. 693-696, doi: 10.1109/ICUFN.2018.8436643.

[4] S. Cui, M. R. Asghar and G. Russello, "Multi-CDN: Towards Privacy in Content Delivery Networks," in IEEE Transactions on Dependable and Secure Computing, vol. 17, no. 5, pp. 984-999, 1 Sept.-Oct. 2020, doi: 10.1109/TDSC.2018.2833110.

[5] Sanjay, B. Rajendran and P. Shetty D., "DNS Amplification & DNS Tunneling Attacks Simulation, Detection and Mitigation Approaches," 2020 International Conference on Inventive Computation Technologies (ICICT), 2020, pp. 230-236, doi: 10.1109/ICICT48043.2020.9112413.

[6] Z. Wu, J. Zhang, W. Xie and F. Yang, "CDN Convergence Based on Multi-access Edge Computing," 2018 10th International Conference on Wireless Communications and Signal Processing (WCSP), 2018, pp. 1-5, doi: 10.1109/WCSP.2018.8555887.

[7] M. Klymash, O. Shpur, N. Peleh, O. Lavriv, R. Bak and O. Skybinskyi, "Increasing the Accessibility of Static Content using CDN Networks as PaaS," 2019 IEEE 15th International Conference on the Experience of Designing and Application of CAD Systems (CADSM), 2019, pp. 1-4, doi: 10.1109/CADSM.2019.8779327.

[8] T. -W. Um, G. M. Lee and H. -W. Lee, "Trustworthiness management in sharing CDN infrastructure," 2018 International Conference on Information Networking (ICOIN), 2018, pp. 73-75, doi: 10.1109/ICOIN.2018.8343088.

基於 PUF 之電子投票系統
(Electronic voting system based on Physically Unclonable Function)

李國誠[1] 朱軒平[2] 戴文諺[3*] 黃政嘉[4]
國立臺灣科技大學資訊管理系[1, 2, 3, 4]
legalcheng23@gmail.com[1]
andy12836@gmail.com[2]
M10909119@mail.ntust.edu.tw[3]
jhengjia.huang@mail.ntust.edu.tw[4]
(*:通訊作者)

摘 要

任何民主國家必然會舉行各種大大小小的選舉以獲得政府治理的正當性。傳統的紙本投票確保了投票時的安全性及合法性，但其背後需要投入大量的人力在開票及驗票上。以美國為例，總統大選的完成開票時間往往從十小時起跳，甚至到數天才結束開票也不為過。本研究旨在將昂貴的傳統投票方法數位化。使用 PUF 技術加強系統底層硬體安全。結合 PUF 的輕量級能力，降低了傳統投票的成本。基於硬體安全防護技術，本計畫的研究基礎仍是要求選民在特定的投票地點進行投票，以保證安全可靠的投票環境。

關鍵詞：PUF(Physically Unclonable Function)物理不可複製函數、SRAM PUF、硬體安全(Hardware Security)、挑戰-響應認證(Challenge-Response authentication)、電子投票(Electronic Voting)

1. 前言

投票是一項人們表達自身意見的重要管道。小從學校或公司內部的意見決定，大至憲法保障人民的選舉與罷免權，都可以看出投票活動的便利性與普遍性。其中，投票活動又以首長選舉最為盛大，最近一次的總統、副總統投票人數超過 1,446 萬人次，投票率超過 74%。然而，對於傳統的投票形式而言，大量的投票人次可能導致舉行選舉的成本過高，如選舉公報的印製與發放、投票會場的人力派遣、以及開票與驗票的人事成本。

在這科技進步的時代，幾乎所有事物都趨向數位化，也因這幾年臺灣數位身分證備受討論，本研究就將重點放在了電子化投票。電子化投票技術已備受討論許久，更有諸多國家開始想將電子投票取代原先的傳統投票，想改善傳統投票帶來的人力問題、成本問題等。迄今已有許多學者提出了對於投票流程的資訊加密方法與模型，如利用區塊鏈進行電子投票[3]，但最後都因有資訊安全問題而沒有被廣泛使用，因此本項研究將以一種不同的角度切入問題，希望從硬體加密的層面探討個資安全的可能性。

藉由檢視過往的電子投票紀錄以闡述本研究重點，台灣大學在校園舉行的學生會投票，整個電子投票過程皆已精心設計。然而，自實施以來的六年中，已有四項技術失敗和學生證驗證失敗等困難。台大學生多次質疑不公平選舉，包括票數錯誤和一人投多票。加上國外有些許國家已經進行了電子投票的測試，包含小型測試或國家規模的試驗，但多數最後仍因安全考量無疾而終。

本研究將 PUF(Physically Unclonable Function)技術融合進電子投票。這項技術應用了物理上的特性，利用電子元件在製造過程中產生的工藝變化做為元件的特徵，並以此做為不可複製的辨識要件。這個特徵就像是人類的指紋，獨一無二不可被複製與預測，再以此特徵保護投票者資料，會是確保資訊安全的一項重要方案。

2. 文獻回顧

本研究的關鍵技術在於物理不可複製函數、加密演算法、挑戰-響應認證。

2.1 PUF(Physically Unclonable Function)

物理不可複製函數(Physically unclonable function, PUF)，是利用硬體在生產時產生的不可預期的小誤差做為特徵，並以此作為辨識該元件的獨特標籤。以一個簡化的舉例說明，在生產電路時提供兩條相同的路徑使電流通過，並標記若電流偏向某一邊的路徑，則紀錄為 1 或是為 0。然而由於製程因素，必無法確保每次都能做出兩條完全相同的路徑。儘管是可接受範圍內的誤差，也會讓每個被製造出的電路擁有不一樣的特性，有些偏向產生 1 的結果，有些產生 0 的結果。

本研究參考了一篇來自荷蘭台夫特理工大學[5]對於 PUF 晶片實作的論文。該論文首先說明了目前使用靜態隨機存取記憶體(SRAM)作為實現 PUF 元件的技術常受限於擁有專利技術的公司或組織，而較少有公開的技術可以使用。因此，若較小型的公司有使用 SRAM PUF 的需求，就有可能受制於取得成本高昂轉而尋求其他可能的解決方案。這項困境也是該論文想要解決的問題，希望能發展出以開源(open source)的形式利用市面上可取

得的 SRAM 晶片完成對 PUF 的需求。

SRAM PUF 原理是在於測量一個未初始化的 SRAM 區塊(block)的啟動值(start-up value)。下圖 2-1 是單個 SRAM 單元的啟動行為，右下方晶體管的閾值電壓低於左下方晶體管的閾值電壓時，儲存在單元格中的結果值為零，反之。

本研究就設定一個閥值電壓來界定 0 和 1 以建立一個 SRAM 矩陣，此矩陣就能達到辨識的效果。圖 2-2 所示。

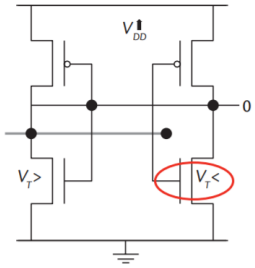


圖 2-1 SRAM 單元啟動行為[4]

圖 2-2 上電後的 SRAM 陣列[4]

2.2 加密演算法

本項研究利用 SHA(Secure Hash Algorithm)密碼散列函數去進行 hash。下圖為 SHA-2 的加密迴圈構造。

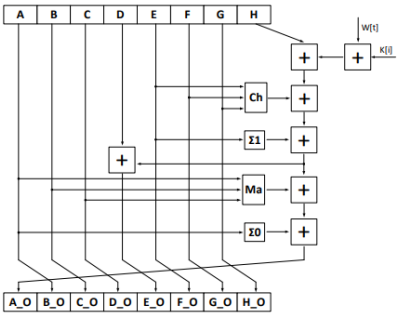


圖 2-3 SHA256 和 SHA512 的加密迴圈[6]

2.3 挑戰-響應認證

挑戰-響應身份驗證在計算機安全上是一組協議，其中一方提出問題「挑戰」，另一方必須提供有效答案-「響應」驗證。挑戰-響應協議的最簡單示例是密碼驗證，其中挑戰是要求輸入密碼，而有效的響應是正確的密碼。可以竊聽密碼進行身份驗證的對手可以以相同的方式對自己進行身份驗證。一種解決方案是發出多組密碼，每組密碼都標有一個標識符。 驗證者可以要求任何密碼，並且證明者必須具有該標識符的正確密碼。 假設密碼是獨立選擇的，攻擊者攔截了一個挑戰-響應消息對沒有線索可以幫助在不同的時間應對不同的挑戰。

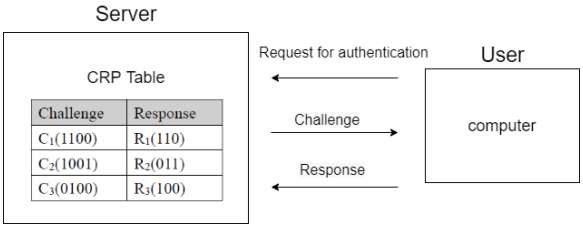


圖 2-4 挑戰-響應認證

本研究利用韓國電子通訊研究院所設計 PUF 在物聯網下認證的機制圖 2-5 所示[1]。來當作基礎去建設系統，針對此機制去做更完善的架構。

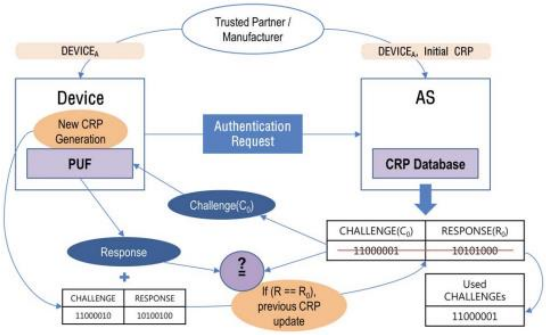


圖 2-5 PUF 認證

3. 研究方法

本研究將方法流程步驟化，取得 PUF 值、建立投票系統、驗證方式。

3.1 取得 PUF 值

本研究採用型號 CY62256NLL 之 SRAM 以取樣 PUF 值。圖 3-1 與 3-2 為此 SRAM 的針腳說明。首先將 WE，CE，OE 等腳位設定為輸出模式，再對 A_0 至 A_{14} 腳位寫電壓(高或低)，即可從 I/O 針腳讀取輸出值。取樣之數值為類比訊號，利用與閾值之電壓比較將類比訊號轉為數位訊號。

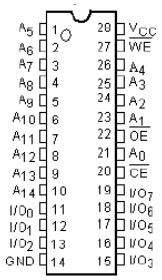


圖 3-1 CY62256NLL 腳位[2]

Pin Number	Type	Description
1–10, 21, 23–26	Input	A_0–A_{14}. Address Inputs
11–13, 15–19,	Input/Output	I/O_0–I/O_7. Data lines. Used as input or output lines depending on operation
27	Input/Control	**WE**. When selected LOW, a WRITE is conducted. When selected HIGH, a READ is conducted
20	Input/Control	**CE**. When LOW, selects the chip. When HIGH, deselects the chip
22	Input/Control	**OE**. Output Enable. Controls the direction of the I/O pins. When LOW, the I/O pins behave as outputs. When deasserted HIGH, I/O pins are tristated, and act as input data pins
14	Ground	**GND**. Ground for the device
28	Power Supply	V_{CC}. Power supply for the device

圖 3-2 CY62256NLL 腳位定義[2]

研究將以 Arduino Mega 取得 PUF 值，下表為開發腳位對應圖。

Arduino Mega2560	SRAM(CY62256NLL)
PIN_2	PIN_21
PIN_3	PIN_23
PIN_4	PIN_24
PIN_5	PIN_25
PIN_6	PIN_26
PIN_22	PIN_1
PIN_24	PIN_2
PIN_26	PIN_3
PIN_28	PIN_4
PIN_30	PIN_5
PIN_32	PIN_6
PIN_34	PIN_7
PIN_36	PIN_8
PIN_38	PIN_9
PIN_40	PIN_10

表 3-1 Selection line 腳位對應圖

Arduino Mega2560	SRAM(CY62256NLL)
A0	I/O 0
A1	I/O 1
A2	I/O 2
A3	I/O 3
A4	I/O 4
A5	I/O 5
A6	I/O 6
A7	I/O 7

表 3-2 data line 腳位對應圖

Arduino Mega2560	SRAM(CY62256NLL)
52	27
48	20
50	22

表 3-3 control 腳位對應圖

Arduino Mega2560	SRAM(CY62256NLL)
5V	28(VCC)
GND	14(GND)

表 3-4 Power 腳位對應圖

利用 Arduino Mega 寫入電位給 SRAM 可產生類比訊號，再經過類比-數位轉換後，產生可用的 bits，就可產生本研究所需的 PUF 值。下圖 3-3 為本研究所取出 2048 位元之 PUF 值陣列，高於閥定電壓為 1(黑色)，反之則為 0(白色)。

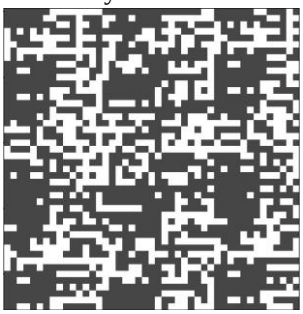


圖 3-3 PUF 值陣列

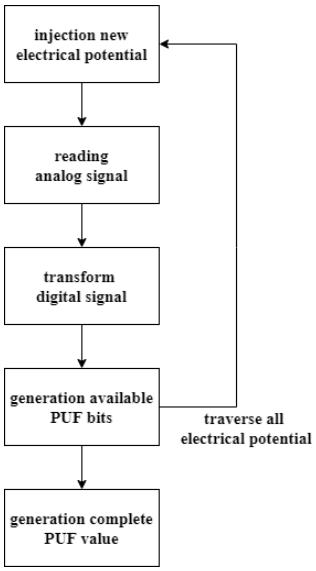


圖 3-4 取得 PUF 值流程

3.2 建立投票系統

本研究設計之架構是將資料與 PUF 合併進行雜湊，以確保資料不可逆推。將投票者與被投票者各進行一次 PUF 加密運算後合併，合併後的結果再進行一次加密，將結果傳回伺服器加以驗票。圖 3-5 所示。

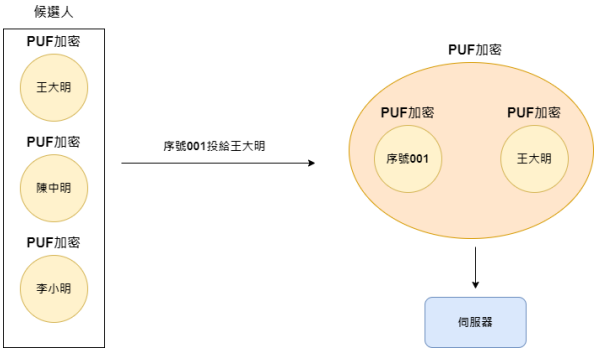


圖 3-5 PUF 加密投票架構

投票系統流程說明如下：(圖 3-6 所示)

1. 投票者持具有身分辨識功能之感應卡進入投票場域，並掃描感應機以開始投票
2. 若投票者符合投票資格且尚未投票，則可成功進入投票畫面；反之則系統顯示投票失敗，不允許投

票者投票。

3. 符合資格的投票者選擇支持者送出後，系統將自我驗證，確認目前運作的正確性。

4. 最後，系統會加密投票人與被支持者的敏感資料，並寫入資料庫。

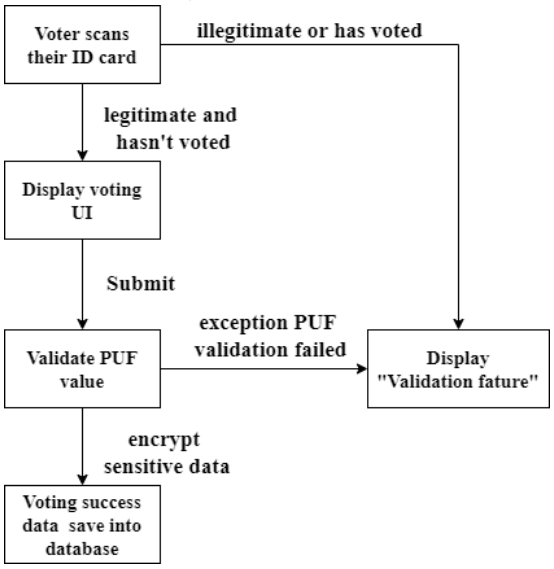


圖 3-6 投票系統流程

圖 3-7 記錄了單次投票紀錄的結果，包含加密後的使用者辨識資料，以及候選人及支持者的 PUF 數值。

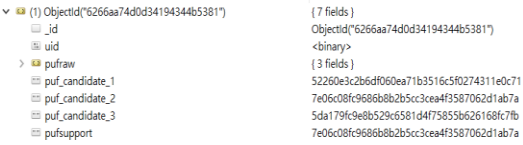


圖 3-7 PUF 加密投票後的結果

3.3 驗證方式

可驗證性對於投票系統是必須的基本要求，本研究系統可以實現兩種驗票機制：

3.3.1 候選人要求驗票。候選人可以要求檢查所有候選人的虛擬投票箱內的選票，此時系統會重新運算資料庫內的每一筆投票紀錄，再計算各候選人之得票結果。由於資料庫內的資料皆有經過加密，因此只有在取得原始 PUF 數值下才能運算解密出投票紀錄，下圖所示。

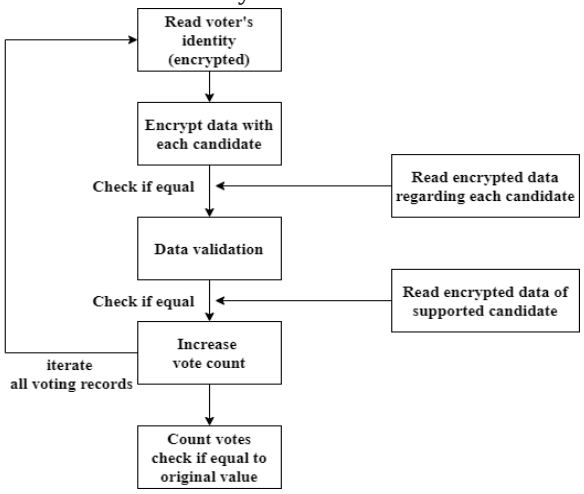


圖 3-7 第一套驗證流程

3.3.2 投票者要求驗票。若投票者對投票系統有疑慮，希望確認當初投下的票是否有正確地被計算。此時投票者可以親自前往投票所重新進行一次模擬投票，若模擬投票的投票結果確實存在於候選人的投票箱內，代表該票有被正確的紀錄，下圖所示。

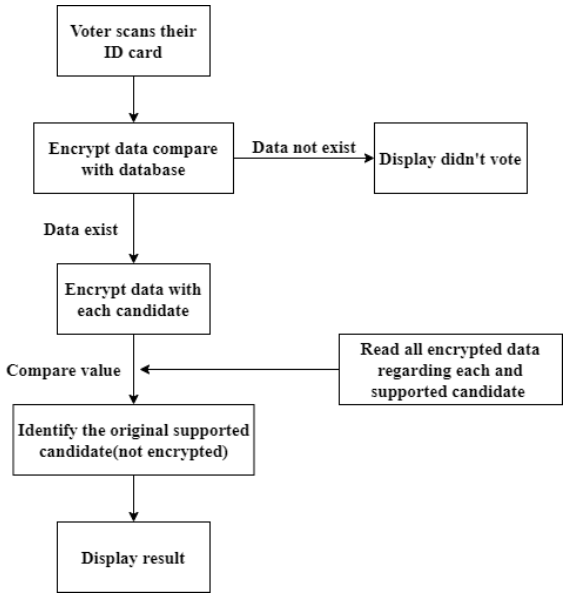


圖 3-8 第二套驗證流程

4. 結論

本研究試圖從硬體安全之層面補足過往電子投票所遭遇的資訊安全議題，並因此導入了新興的 PUF 技術做為取得加密過程之重要因子。本篇論文最後亦顯示了此方法的可行性，其許可作為電子投票實行時的一項參考。

參考文獻

[1] B. Kim, S. Yoon, Y. Kang and D. Choi, "PUF based IoT Device Authentication Scheme," 2019 International Conference on Information and

Communication Technology Convergence (ICTC), 2019,pp.1460-1462,doi:10.1109/ICTC46691.2019.8939751.

[2] Cypress, (2017), “001-06511 Rev. *J”[PDF file].

[3] F. D. Giraldo, B. Milton C. and C. E. Gamboa, "Electronic Voting Using Blockchain And Smart Contracts: Proof Of Concept," in IEEE Latin America Transactions, vol. 18, no. 10, pp. 1743-1751,October2020,doi:10.1109/TLA.2020.9387645.

[4] Helena Handschuh | Katholieke Universiteit Leuven ,Hardware-Anchored Security Based on SRAM PUFs, Part 1 Page(s): 80 - 83 Date of Publication:26,June,2012 DOI:10.1109/MSP.2012.68

[5] Sajim,Ade Setyawan. “Open-Source Software-Based SRAM-PUF for Secure Data and Key Storage Using Off-The-Shelf SRAM.” (2018).

[6] S. Brazhnikov, "A Hardware Implementation of the SHA2 Hash Algorithms Using CMOS 28nm Technology," 2020 IEEE Conference of Russian Young Researchers in Electrical and Electronic Engineering (EIConRus), 2020, pp. 1784-1786, doi: 10.1109/EIConRus49466.2020.9039083.

專題通過科技部(現國科會)大專生計畫

111	朱軒平	國立臺灣科技大學資訊管理系	計畫名稱：基於PUF(Physically Unclonable Function)之電子投票系統 計畫編號：111-2813-C-011-007-E 成果報告：無電子檔 執行起迄：2022/07/01~2023/02/28 指導教授：黃政嘉 核定金額：58,000元

工程技術司

計畫名稱：基於 PUF(Physically Unclonable Function)之電子投票系統

計畫編號：111-2813-C-011-007-E

執行起迄：2022/07/01~2023/02/28

指導教授：黃政嘉

國立臺灣科技大學資訊管理系 專題貢獻度:

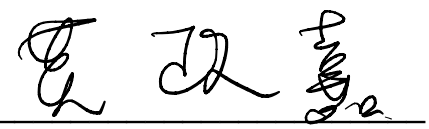
組員: 李國誠 朱軒平

組員	貢獻百分比
李國誠	50%
朱軒平	50%

分工: 由於本組只有少數的兩人，並未明確分工，在專題製作、撰寫論文以及計劃書幾乎都是一起執行，相互研究、合作、討論產生出來的，因此表格內並無分工內容。

指導教授: 黃政嘉 助理教授

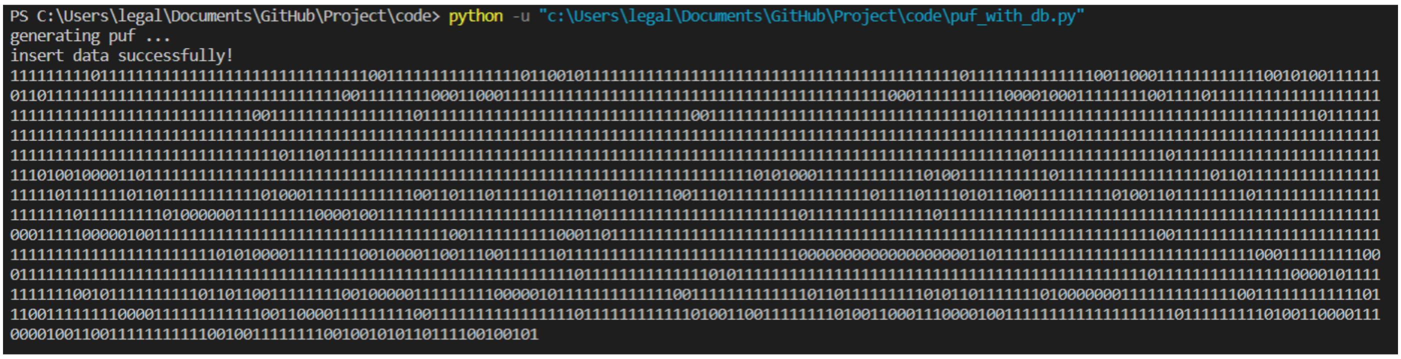
單位: 國立臺灣科技大學 資訊管理系

簽名: 

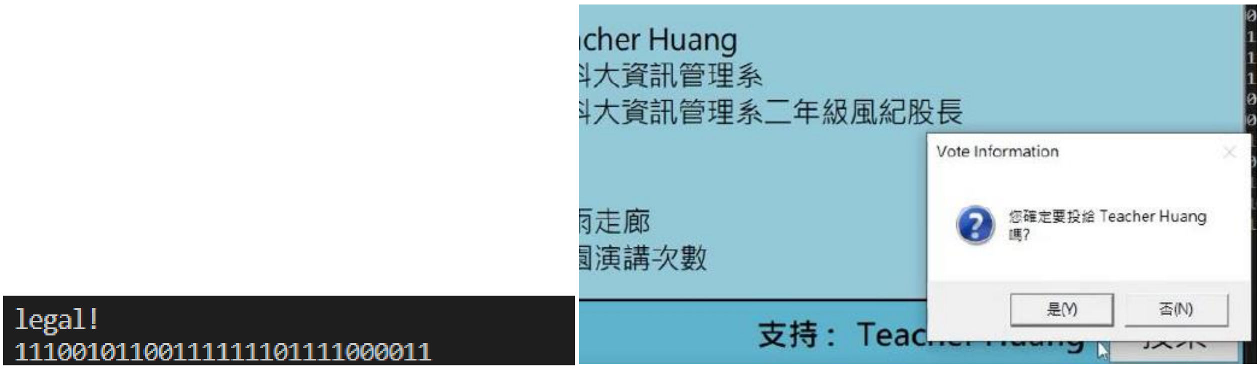
論文延伸-專題實作系統:

在上述論文以學術角度去探討 SRAM PUF 硬體加密應用在電子化流程上，並未展示其系統成果，因以此頁為專題實作系統展示。

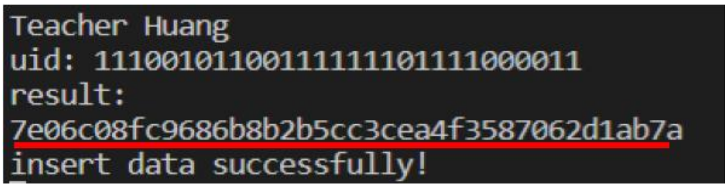
1. 為最初生成 PUF 值 - 共 2048 位元



2. 以 PUF 值與合法身分者進行雜湊演算並會將被投票者一起進行雜湊。



3. 雜湊完的數值會先進行比對，確認其 PUF 值是指定機器所送出的，因 PUF 值具有唯一性，若無法成功存入資料庫內，代表其 PUF 值為錯誤，反之成功。



4. 研究過程

   本專題在設計過程其實面臨非常多困難，光是去尋找如何將硬體之間的不定數取出，就研究了非常多的時間，也在暑假期間定時與指導老師與一些碩士班學長姊去討論如何將本系統所需要的值拿出來使用，討論好之後也需要訂晶片去做測試，花費了大概快半年才將我們所需要的值給取出，但也因為 PUF 的一些外在因素，例如溫度濕度，都會影響 PUF 的穩定性，也屬實困擾到我們，不過後來也將這個穩定性排除後就差不多完成我們的投票系統。

5. 未來展望

   本專題成功地提出了一項以 PUF 作為加密元件的電子投票系統之原型，但仍有些許地方尚有不足，期望能在未來進行強化及擴充。比如本系統目前僅以一台電腦作為投票機器，尚未以多台電腦同時投票納入實作以及本系統採用 RFID 感應學生證作為身分辨識之依據，然而以現實考量，目前有許多更具安全性之辨識方法，如指紋辨識，皆可取代以感應卡作為辨識方法。因此本專題認為，未來的改進目標可著重於上述兩點，使本投票系統更與穩定及安全性。

主題: IoT Zeroday

摘要: 針對地震儀進行相關檢測，其發現同系列型號與受測物韌體內容相同且在某些監測單位依然還在使用。

其發現漏洞:

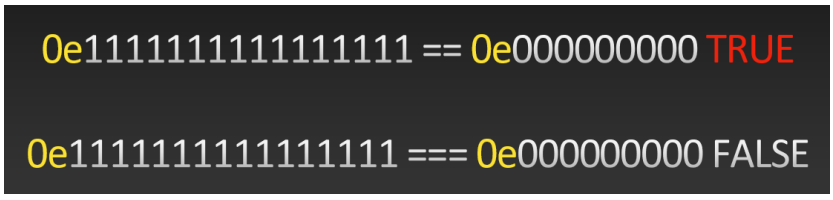
1. **PHP version 及 Linux version 版本過舊(有諸多 CVE 漏洞)**

2. **LFI, Local File Inclusion (本地檔案引入漏洞)**
   透過此漏洞可去路徑下爬到原始碼資料，進而可以進行白箱測試 (原始碼檢測)

3. **Command Injection (命令注入攻擊)**
   檢視原始碼在某 php 檔中發現使用危險函數 shell_exec()，透過引號先將前面程式封閉起來，再輸入簡單後門程式 <?php system($_GET["cmd"]); ?>，再進行封閉就成功寫入後門程式，在網頁中執行後門程式可直接對地震儀進行後台控制。

4. **Arbitrary File Upload (任意檔案上傳漏洞)**
   在上傳檔案的程式碼當中，並沒有驗證檔案的副檔名、Content-type 或是檔案內容等，可直接上傳任意檔案，也一樣植入簡易後門程式就能操控後台。

5. **Logic Flaws (邏輯缺陷)**
   密碼有進行 md5 雜湊，即使 md5 現可利用撞表方式已不安全，但不已明文傳輸密碼具備一定安全性。在舊 PHP 版本有邏輯判斷的問題存在，如果透過兩個等於(==)判斷會將具有科學記號的任意雜湊後數值判斷為 0，必須用三個等於判斷(===)才會將科學記號考慮進去，因為我們時常撰寫程式都會利用兩個等於去判斷，所以這是在舊版本開發者常忽略到的問題。
   註: PHP 新版本已修正這個邏輯缺陷

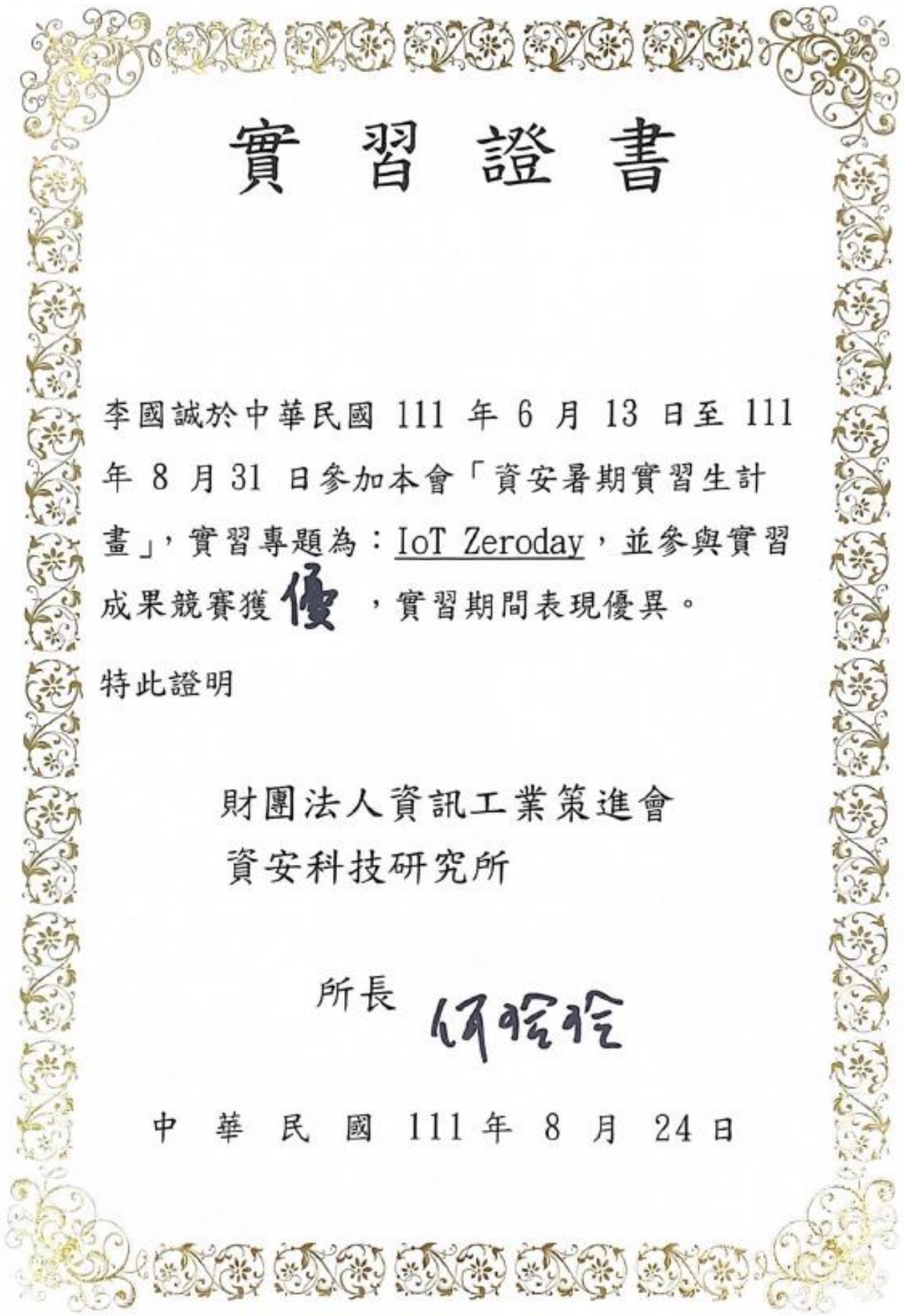


6. **Privilege Escalation (提權)**
   跑 PEASS-ng 套件可發現相關 CVE 漏洞，此 CVE 在 github 上搜索，就可以透過此 CVE 進行提權的動作。

此計畫當中，可以使自己的擅長的項目一展身手，不僅僅是對於此主題，在其他物聯網設備檢測專案當中也學習到相當多知識以及能力，透過此計畫使自己在資訊安全領域成長且更有熱忱。

註: 此頁報告未透漏任何廠商任何設備的相關資訊，也未是公司的廠商專案，所以並不影響公司及廠商權益，但此頁報告只僅限推甄資料使用，未公開在網路上。

證書:



實 習 證 書

李國誠於中華民國 111 年 6 月 13 日至 111 年 8 月 31 日參加本會「資安暑期實習生計畫」，實習專題為：IoT Zeroday，並參與實習成果競賽獲 優 ，實習期間表現優異。

特此證明

財團法人資訊工業策進會
資安科技研究所

所長 何俊欣

中 華 民 國 111 年 8 月 24 日

專題主題: CAN bus 模擬車輛劫持

背景內容:

CAN (Controller Area Network)

1. ECU 之間傳輸資料的 通訊協定。
2. 著重於資料可靠性，預防不可預測行為。
   Safety 不著重安全性，人為的攻擊行為。
   Security 不考量安全性是因為早期車輛為封閉系統。
3. 早期通過實體 的 OBD II port 存取 CAN Bus
   現代 OBD II 有了藍芽或是 LTE 等等存取方式，車輛不再是一個封閉系統。
   車輛系統為封閉系統的前提漸漸地被打破能通過外部的手段存取內部網路。

進行的攻擊手法:

對目標汽車 CAN Bus 封包進行竄改或注射。

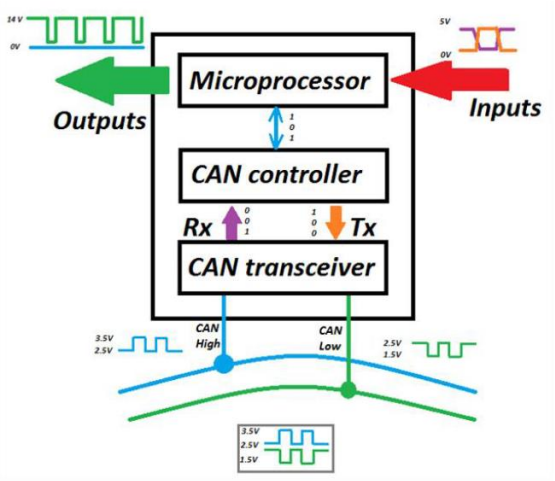
HOW TO WORK ?

CAN 設計為確保資料完整性，因此有一些檢查的手法，像是 CRC 錯誤檢驗，竄改封包會導致封包無法進入 CAN bus，需要通過一些特殊裝置直接連接到 Tx 與 Rx 才能夠實現，也就是需要一些物理方法。

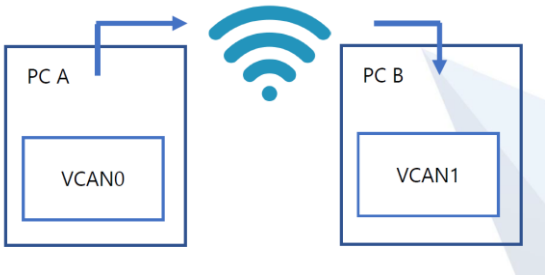
每個 Frame 會在 CAN Bus 上廣播讓每個裝置都會收到 Frame 且這個 Frame 是沒有經過加密的。

只需要讓汽車的某個部件使用雙絞線連接到 CAN Bus 即可看見明文封包進行分析。

任意 ECU 可以使用任意 ID 將封包藉由 CAN Bus 發送到目標，而如果兩個封包具有相同的 ID 則目標將無法辨認該封包是來自於哪 一個 ECU 或是攻擊者。



簡易的想法?



Live Demo (現場展示)

-實際模擬車輛接收到的訊號，利用一台電腦送訊號給另一台電腦進而達到劫持操控。

參考資料:

- Comprehensive Experimental Analyses of Automotive Attack Surfaces
- Automobile CAN Bus Network Security and Vulnerabilities
- Development of a Man in the Middle Attack Device for the CAN Bus
- The Car Hacker's Handbook A Guide for the Penetration Tester (Craig Smith)
- Blackhat Remote Exploitation of an Unaltered Passenger Vehicle

證書:

教育部先進資通安全實務人才培育計畫
AIS3新型態資安暑期課程

合格證明

李國誠 君

111年7月25日至7月31日參加 教育部先進資通安全實務人才培育計畫
111年度產業專題導向新型態資安暑期課程共計40小時，
修習成績及格，特頒此證書。

教育部先進資通安全實務人才培育計畫辦公室

吳宗成 Tzong-Chen Wu　　鄭欣明 Shin-Ming Cheng
黃俊穎 Chun-Ying Huang　　王銘宏 Ming-Hung Wang
蕭旭君 Hsu-Chun Hsiao　　陳昱圻 Yu-Chi Chen

教育部 推動辦公室 資通安全實務人才培育計畫

中華民國 111 年 7 月 31 日

ISIP-AIS3 2022-合-137

第 26 屆全國資訊服務創新競賽 資安組決賽

連結:

https://innoserve.tca.org.tw/qanda.aspx

凡入圍決賽有提供入圍證明的組別只有AIoT創新應用組(TQC+)、商業資訊創新應用組(GCIS-OPENDATA)、耐能邊緣運算AI運用組(Kneron)，若不在上述組別請以報名確認信當作參賽證明。

2022/9/26 晚上10:03 Gmail - Re: 2021第26屆InnoServe大專校院資訊應用服務創新競賽 決賽入圍通知

Gmail 李國誠 <kk787826@gmail.com>

Re: 2021第26屆InnoServe大專校院資訊應用服務創新競賽 決賽入圍通知

1 封郵件

朱軒平 <andy12836@gmail.com> 2021年10月25日 晚上7:01
收件者: "kk787826@gmail.com" <kk787826@gmail.com>

InnoServe大專校院資訊應用創新競賽委員會 <pt3561@image.tca.org.tw> 於 2021年10月25日 週一 16:21 寫道：

2021第26屆InnoServe大專校院資訊應用服務創新競賽

決賽入圍通知

首先恭喜團隊入圍11月6日（六）決賽!!

今年因考量COVID-19疫情尚未穩定，及本競賽參與人數眾多，為顧及所有參賽團隊及評審委員的安全，故今年競賽將採「全線上」方式辦理。

決賽分組名單及編號(附件一)資訊已於10月25日(一)中午12:00公布於「2021第26屆大專校院資訊應用服務創新競賽」官網https://reurl.cc/GbnqX3，並將再以E-mail通知團隊。

為使11/6(六)線上決賽順利進行，請入圍決賽團隊配合以下事項：

一、 決賽須知

（一）請團隊務必於10/26(二)中午12:00前回填以下兩個連結表單：

1. 決賽團隊視訊系統前測-時間調查問卷：https://seminars.tca.org.tw/D15p01825.aspx

※當日測試重點，請詳見「二、線上競賽原則之(二) Webex視訊系統前測說明」

2. 線上決賽聲明書：https://seminars.tca.org.tw/D15p01858.aspx

（二）決賽時間：110年11月6日(星期六)，須依「各梯次團隊報到時間」準時上線

（三）參與對象：團隊線上報到時，所有團隊成員均須「出示學生證」，大會將進行身分查驗並截圖存查。(指導老師及非團隊成員不得參與線上競賽)

（四）Webex視訊系統登入者：每個團隊「至多使用4個帳號登入」Webex視訊系統，為使線上競賽進行順暢，「參與系統前測」及「線上決賽當日」負責操作及登入Webex視訊系統之同學，須為同一人。

（五）線上競賽網址：將於決賽行前通知告知。

https://mail.google.com/mail/u/2/?ik=56ddce9911&view=pt&search=all&permthid=thread-f%3A1714589196703735278&simpl=msg-f%3A1714589... 1/4

第七屆臺灣好厲駭 資安培訓計畫 高階培訓學員證明:

Gmail 李國誠 <kk787826@gmail.com>

【第七屆臺灣好厲駭】錄取與面試通知

3 封郵件

彤琳 <icelandrmp@gmail.com> 2022年9月13日 晚上7:35
密件副本: kk787826@gmail.com

同學您好：

恭喜您『通過』教育部先進資通安全實務人才培育計畫-111年度資安實務導師制度~臺灣好厲駭-培訓學員徵選。

由於您所提供的資料顯示您已經具備相當程度的資安技術，因此導師審查中一致決議推薦您能參與複審口試。如果通過複審口試，您將有機會與導師進行媒合，媒合成功可與導師討論您的培訓計畫與主題，並接受導師的親自指導。若面試未通過或媒合不成，您還可參與高階培訓模式。

兩種培訓模式說明：

(1)高階培訓模式

- 通過第一階段初選者即可參與。
- 由計畫辦公室舉辦之系列強化培訓課程，由資深學員及導師進行不同主題的資安實務與CTF培訓。
- 部分高階培訓課程為有利於學習，需要學員完成基本測驗，測驗通過後始得參加培訓課程。
- 參與高階培訓模式學員其期末結業評審將由計畫辦公室彙整學員期末培訓報告提交導師會議決議。

(2)導師深度輔導模式

- 需通過第二階段面試且經導師媒合成功者。
- 除可參與高階培訓模式課程外，可參加導師深度輔導。
- 資安實務導師經由媒合機制選定欲培訓的學員，培訓學員依資安實務導師所訂立之培訓目標以師徒制方式進行培訓。
- 培訓的方式由資安實務導師及學員共同擬定研究主題，由學生**主動**進行研究並由導師輔導進度與技術，但各培訓導師可依培訓領域的特殊性、學生既有能力與興趣專長等實際狀況進行調整。
- 參與導師深度輔導模式學員其期末結業將由導師進行審查評分。

本計畫辦公室於111年9月18日(日)9:30~15:30安排線上導師口試會，面試時間表如下：

姓名	面試時間
邱□森	09:40-09:50
楊□旭	09:50-10:00

KPMG 安侯企業 數位安全部 資安技術研究員

Gmail 李國誠 <kk787826@gmail.com>

KPMG<數位科技安全實務應用實習生>人才徵選計畫 - 錄取通知

4 封郵件

Wang, Christina I.H. (TW/319319) <christinawang@kpmg.com.tw> 2022年6月17日 下午4:51
收件者: "kk787826@gmail.com" <kk787826@gmail.com>
副本: "Hsieh, Jason Y.T. (TW/300300)" <jasonhsieh@kpmg.com.tw>, "Hsiu, David S.C. (TW/319319)" <dhsiu@kpmg.com.tw>

李國誠同學您好：

恭喜您在激烈的競爭中脫穎而出，成為本次KPMG<數位科技安全實務應用實習生>徵選的正取人選。報到日期為2022/7/4(一)，報到地點在台北101辦公大樓68樓，請檢視下列僱用條件，若沒有問題請填寫附件「職位申請表」簽名後回傳，後續將由HR進行聘僱作業，若有其他問題請於下週一中午12:00前回覆，謝謝！

- 應徵職缺：資訊安全技術專案實習生

Best regards,

王宜慧 Christina Wang

經理，數位安全顧問服務

Manager, Cybersecurity Services

KPMG 安侯企業管理股份有限公司

台北市110615信義路5段7號68樓(台北101大樓)
TAIPEI 101 TOWER, 68F, No.7, Sec. 5, Xinyi Rd.,
Taipei City 110615, Taiwan (R.O.C.)

T +886 2 8101 6666 ext.10285

F +886 2 8101 6667 ext.10285